PUBLISHED

UNITED STATES COURT OF APPEALS

FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v. No. 99-4238

MARK L. SIMONS,
Defendant-Appellant.

Appeal from the United States District Court
for the Eastern District of Virginia, at Alexandria.
James C. Cacheris, Senior District Judge.
(CR-98-375)

Argued: November 30, 1999

Decided: February 28, 2000

Before WILKINS and NIEMEYER, Circuit Judges, and Margaret B. SEYMOUR, United States District Judge for the District of South Carolina, sitting by designation.

Affirmed in part and remanded in part by published opinion. Judge Wilkins wrote the opinion, in which Judge Niemeyer and Judge Seymour joined.

COUNSEL

ARGUED: Marvin David Miller, LAW OFFICES OF MARVIN D. MILLER, Alexandria, Virginia, for Appellant. G. David Hackney, Assistant United States Attorney, UNITED STATES ATTORNEY'S OFFICE, Alexandria, Virginia, for Appellee. **ON BRIEF:** Helen F.

Fahey, United States Attorney, UNITED STATES ATTORNEY'S OFFICE, Alexandria, Virginia, for Appellee.

OPINION

WILKINS, Circuit Judge:

Mark L. Simons appeals his convictions for receiving and possessing materials constituting or containing child pornography, see 18 U.S.C.A. § 2252A(a)(2)(A), (a)(5)(B) (West Supp. 1999). Simons, who received the unlawful materials at his government workplace via the Internet, argues that the district court erred in denying his motion to suppress. We affirm in part and remand in part.

I.

Simons was employed as an electronic engineer at the Foreign Bureau of Information Services (FBIS), a division of the Central Intelligence Agency (CIA). FBIS provided Simons with an office, which he did not share with anyone, and a computer with Internet access.

In June 1998, FBIS instituted a policy regarding Internet usage by employees. The policy stated that employees were to use the Internet for official government business only. Accessing unlawful material was specifically prohibited. The policy explained that FBIS would conduct electronic audits to ensure compliance:

> Audits. Electronic auditing shall be implemented within all FBIS unclassified networks that connect to the Internet or other publicly accessible networks to support identification, termination, and prosecution of unauthorized activity. These electronic audit mechanisms shall . . . be capable of recording:
>
> - Access to the system, including successful and failed login attempts, and logouts;

- Inbound and outbound file transfers;

- Terminal connections (telnet) to and from external systems;

- Sent and received e-mail messages;

- Web sites visited, including uniform resource locator (URL) of pages retrieved;

- Date, Time, and user associated with each event.

J.A. 125-26. The policy also stated that "[u]sers shall . . . [u]nderstand FBIS will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate." J.A. 127.

FBIS contracted with Science Applications International Corporation (SAIC) for the management of FBIS' computer network, including monitoring for any inappropriate use of computer resources. On July 17, 1998, Clifford Mauck, a manager at SAIC, began exploring the capabilities of a firewall recently acquired by SAIC, because Mauck believed that SAIC needed to become more familiar with the firewall to service the FBIS contract properly. **1** Mauck entered the keyword "sex" into the firewall database for July 14 and 17, 1998, and found a large number of Internet "hits" originating from Simons' computer. It was obvious to Mauck from the names of the sites that they were not visited for official FBIS purposes.

Mauck reported this discovery to his contact at FBIS, Katherine Camer. Camer then worked with another SAIC employee, Robert Harper, to further investigate the apparently unauthorized activity. Camer instructed Harper to view one of the websites that Simons had visited. Harper complied and found that the site contained pictures of nude women.

---

1 A firewall is like a funnel through which all Internet access flows and is registered; the firewall collects data and may be searched as a database.

At Camer's direction and from his own workstation, Harper examined Simons' computer to determine whether Simons had downloaded any picture files from the Internet; Harper found over 1,000 such files. Again from his own workstation, Harper viewed several of the pictures and observed that they were pornographic in nature. Also at Camer's request and from his own workstation, Harper printed a list of the titles of the downloaded picture files. Harper was then asked to copy all of the files on the hard drive of Simons' computer; Harper accomplished this task, again, from his own workstation.

On or about July 31, 1998, two representatives from the CIA Office of the Inspector General (OIG), one of whom was a criminal investigator, viewed selected files from the copy of Simons' hard drive; the pictures were of minors. Later that day, Harper physically entered Simons' office, removed the original hard drive, replaced it with a copy, and gave the original to the FBIS Area Security Officer. The Security Officer turned it over to the OIG criminal investigator the same day.**2** This last assignment was the only one that required Harper to physically enter Simons' office.

On August 5, 1998, FBI Special Agent John Mesisca viewed over 50 of the images on the hard drive that had been removed from Simons' office; many of the images contained child pornography. Mesisca, Harper, the two OIG representatives, and Assistant United States Attorney Tom Connolly worked together to prepare an application for a warrant to search Simons' office and computer. An affidavit from Mesisca supported the warrant application. The affidavit stated, inter alia, that Simons had connected a zip drive to his computer.**3** The affidavit also expressed a "need" to conduct the search in secret. J.A. 140.

The warrant was issued on August 6, 1998. It stated that the executing officers were to leave at Simons' office a copy of the warrant and a receipt for any property taken. The warrant mentioned neither permission for, nor prohibition of, secret execution.

---

2 The OIG investigator "placed it into evidence." J.A. 70.
3 A zip drive is a device for storing computer files; it has greater storage capacity than other computer storage devices. Zip drive diskettes work only in zip drives and not with other computer storage devices.

Mesisca and others executed the search during the evening of August 6, 1998, when Simons was not present. The search team copied the contents of Simons' computer; computer diskettes found in Simons' desk drawer; computer files stored on the zip drive or on zip drive diskettes;**4** videotapes; and various documents, including personal correspondence. No original evidence was removed from the office. Neither a copy of the warrant nor a receipt for the property seized was left in the office or otherwise given to Simons at that time, and Simons did not learn of the search for approximately 45 days.**5** When Mesisca reviewed the computer materials copied during the search, he found over 50 pornographic images of minors.

In September 1998, Mesisca applied for a second search warrant. The supporting affidavit, like the affidavit that supported the August application, stated that Simons had connected a zip drive to his computer. The September affidavit described the August application as an application for a surreptitious search warrant.

A second search warrant was obtained on September 17, 1998 and executed on September 23, 1998, with Simons present. Original evidence was seized and removed from the office. The executors left Simons with a copy of the warrant and an inventory of the items seized.

Simons subsequently was indicted on one count of knowingly receiving child pornography that had been transported in interstate commerce, see 18 U.S.C.A. § 2252A(a)(2)(A), and one count of knowingly possessing material containing images of child pornography that had been transported in interstate commerce, see 18 U.S.C.A. § 2252A(a)(5)(B). Simons moved to suppress the evidence, arguing that the searches of his office and computer violated his Fourth Amendment rights. Following a hearing, the district court denied the motion. With regard to the warrantless searches, the district court first concluded that Simons lacked a legitimate expectation of privacy in

---

4 The parties agree that materials associated with the zip drive were copied during the search, but the record is not clear as to whether the materials actually came from the zip drive itself or from zip diskettes. Resolution of this factual matter is not necessary to decide this appeal.
5 A property list was returned to the magistrate judge, as required.

his Internet use. The court nevertheless determined that, even if Simons did have a legitimate expectation of privacy, all of the warrantless searches satisfied the reasonableness requirement of the Fourth Amendment. The district court also upheld the warrant searches.

At a bench trial on stipulated facts, four computer picture files depicting child pornography were introduced as evidence of Simons' guilt. The district court found Simons guilty on both counts and sentenced him to 18 months imprisonment. Simons now appeals, maintaining that the district court erred in denying his motion to suppress.

Inexplicably, the record does not indicate which search or searches yielded the four computer picture files used against Simons at trial. Consequently, we are called upon to review the constitutionality of all of the searches. We consider first the warrantless searches, then turn to Simons' challenges to the searches conducted pursuant to the August search warrant.**6**

II.

The Fourth Amendment prohibits "unreasonable searches and seizures" by government agents, including government employers or supervisors. U.S. Const. amend. IV; see O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (plurality opinion); id. at 730-31 (Scalia, J., concurring in the judgment). To establish a violation of his rights under the Fourth Amendment, Simons must first prove that he had a legitimate expectation of privacy in the place searched or the item seized. See Rakas v. Illinois, 439 U.S. 128, 143 (1978); United States v. Rusher, 966 F.2d 868, 873-74 (4th Cir. 1992). And, in order to prove a legitimate expectation of privacy, Simons must show that his subjective expectation of privacy is one that society is prepared to accept as objectively reasonable. See California v. Greenwood, 486 U.S. 35, 39 (1988).

---

6 Simons also challenges the search conducted pursuant to the September search warrant. We address his arguments with regard to this search infra, in note 12.

Government employees may have a legitimate expectation of privacy in their offices or in parts of their offices such as their desks or file cabinets. See O'Connor, 480 U.S. at 716-18; Shields v. Burge, 874 F.2d 1201, 1203-04 (7th Cir. 1989) (concluding that the holding of the O'Connor plurality governs). However, office practices, procedures, or regulations may reduce legitimate privacy expectations. See O'Connor, 480 U.S. at 717; id. at 737 (Blackmun, J., dissenting). In reviewing a denial of a motion to suppress, we review the factual findings of the district court for clear error and its legal conclusions de novo. See United States v. Johnson, 114 F.3d 435, 439 (4th Cir. 1997).

We first consider Simons' challenge to the warrantless searches of his computer and office by FBIS.**7** We conclude that the remote searches of Simons' computer did not violate his Fourth Amendment rights because, in light of the Internet policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet. Additionally, we conclude that Simons' Fourth Amendment rights were not violated by FBIS' retrieval of Simons' hard drive from his office.

Simons did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of the FBIS Internet policy. The policy clearly stated that FBIS would "audit, inspect, and/or monitor" employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, "as deemed appropriate." J.A. 127. This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private.**8** Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were pri-

---

7 Although an SAIC employee conducted the searches, for ease of reference and in light of the fact that SAIC was an FBIS contractor, we refer to the searches as having been carried out by FBIS.

Also, Simons has focused exclusively on the warrantless nature of these searches; he has not argued that the searches were not supported by probable cause. We therefore limit our discussion to the warrantless nature of the searches.

8 Simons does not assert that he was unaware of, or that he had not consented to, the Internet policy.

vate, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use. **9** See American Postal Workers Union v. United States Postal Serv., 871 F.2d 556, 560 (6th Cir. 1989) (concluding that employees had no reasonable expectation of privacy in lockers in light of policies allowing locker inspections); cf. United States v. Sellers, 667 F.2d 1123, 1126 (4th Cir. 1981) (noting that "whenever one `knowingly exposes his activities [or effects] to third parties, he surrenders Fourth Amendment protections' in favor of such activities or effects" (alteration in original) (quoting Reporters' Comm. for Freedom of the Press v. AT&T , 593 F.2d 1030, 1043 (D.C. Cir. 1978)). Accordingly, FBIS' actions in remotely searching and seizing the computer files Simons downloaded from the Internet did not violate the Fourth Amendment.

We next consider whether Harper's warrantless entry into Simons' office to retrieve his hard drive violated the Fourth Amendment. The district court did not separately address this search; rather, it evaluated all of the warrantless searches together. Although we agree with the district court that Simons lacked a legitimate expectation of privacy in his Internet use, and thus in the hard drive itself, Harper's entry into Simons' office to retrieve the hard drive presents a distinct question. See United States v. Horowitz, 806 F.2d 1222, 1224 (4th Cir. 1986) (describing the appropriate inquiry as"whether the individual had a reasonable expectation of privacy in the area searched, not merely in the items found"); United States v. Manbeck, 744 F.2d 360, 374 (4th Cir. 1984) (stating that "[t]he privacy interest that must be established to support standing is an interest in the area searched, not an interest in the items found"); cf. Horton v. California, 496 U.S. 128, 137 n.7 (1990) ("[E]ven where the object is contraband, this Court has repeatedly stated and enforced the basic rule that the police may not enter and make a warrantless seizure" absent exigent circumstances (internal quotation marks omitted)).

The burden is on Simons to prove that he had a legitimate expectation of privacy in his office. See Rusher, 966 F.2d at 874. Here,

---

9 Simons attempts to distinguish the files downloaded from the Internet from the record of those downloads registered on the firewall, and argues that he had a legitimate expectation of privacy in the former. We decline to recognize the distinction Simons advocates.

Simons has shown that he had an office that he did not share. As noted above, the operational realities of Simons' workplace may have diminished his legitimate privacy expectations. However, there is no evidence in the record of any workplace practices, procedures, or regulations that had such an effect.**10** We therefore conclude that, on this record, Simons possessed a legitimate expectation of privacy in his office.**11**

Consequently, we must determine whether FBIS' warrantless entry into Simons' office to retrieve the hard drive was reasonable under the Fourth Amendment. A search conducted without a warrant issued by a judge or magistrate upon a showing of probable cause is "per se unreasonable" unless it falls within one of the"specifically established and well-delineated exceptions" to the warrant requirement.

---

10 The Internet policy did not render Simons' expectation of privacy in his office unreasonable. The policy does not mention employees' offices, and although it does not prohibit FBIS from carrying out its "audit[ing], inspect[ing], and/or monitor[ing]" activities at employees' individual workstations, J.A. 127, this fact alone is insufficient to render unreasonable an employee's subjective expectation of privacy in his office. Cf. Schowengerdt v. United States, 944 F.2d 483, 485, 488-89 (9th Cir. 1991) (holding that civilian employee of Navy weapons plant lacked legitimate expectation of privacy in private office when office was regularly searched in employee's absence, employee was aware that such searches occurred, and employee had participated in searches of coworkers' offices); United States v. Taketa, 923 F.2d 665, 672-73 (9th Cir. 1991) (rejecting argument that government employee lacked a legitimate expectation of privacy in his office because regulation requiring clean desks implied that office was subject to inspection, in part on ground that the regulation had not been enforced by a practice of inspections).

Although the CIA may have had other policies that rendered unreasonable any expectation of privacy in an office occupied by an employee, such as Simons, with access to classified information, no such policies were made a part of this record and consequently we must assume that none existed.

11 While we are not impressed with the degree to which this issue was factually developed in the district court, remand for further factual development is not appropriate as the issue was clearly raised and both parties had an opportunity to introduce evidence on the matter.

Katz v. United States, 389 U.S. 347, 357 (1967); see United States v. Lattimore, 87 F.3d 647, 650 (4th Cir. 1996) (en banc). One exception to the warrant requirement arises when the requirement is rendered impracticable by a "special needs, beyond the normal need for law enforcement." Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (internal quotation marks omitted). In O'Connor, the Supreme Court held that a government employer's interest in"the efficient and proper operation of the workplace" may justify warrantless work-related searches. O'Connor, 480 U.S. at 723; see id. at 720-25. In particular, the O'Connor Court held that when a government employer conducts a search pursuant to an investigation of work-related misconduct, the Fourth Amendment will be satisfied if the search is reasonable in its inception and its scope. See id. at 725-26. A search normally will be reasonable at its inception "when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct." Id. at 726. "The search will be permissible in its scope when `the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the[misconduct].'" Id. (alterations in original) (quoting New Jersey v. T.L.O., 469 U.S. 325, 342 (1985)).

The question thus becomes whether the search of Simons' office falls within the ambit of the O'Connor exception to the warrant requirement, i.e., whether the search was carried out for the purpose of obtaining "evidence of suspected work-related employee misfeasance." Id. at 723. The district court found that all of the warrantless searches, and thus the office search, were work-related. The court reasoned that FBIS had an interest in fully investigating Simons' misconduct, even if the misconduct was criminal. We agree.

As it does not appear from the record that FBIS utilized the hard drive for internal investigatory purposes before turning it over to the criminal investigator at OIG, we will assume that the dominant purposes of the warrantless search of Simons' office was to acquire evidence of criminal activity, which had been committed at FBIS using FBIS equipment. Nevertheless, the search remains within the O'Connor exception to the warrant requirement; FBIS did not lose its special need for "the efficient and proper operation of the workplace," id., merely because the evidence obtained was evidence of a crime.

Cf. New York v. Burger, 482 U.S. 691, 716 (1987) (holding that "[t]he discovery of evidence of crimes in the course of an otherwise proper administrative inspection does not render that search illegal or the administrative scheme suspect"); Ferguson v. City of Charleston, 186 F.3d 469, 477 n.7 (4th Cir. 1999) (observing that eventual use in a criminal proceeding of evidence obtained during a special needs search does not "preclude[ ] application of the special needs balancing test"), petition for cert. filed, 68 U.S.L.W. 3391 (U.S. Dec. 1, 1999) (No. 99-936). Simons' violation of FBIS' Internet policy happened also to be a violation of criminal law; this does not mean that FBIS lost the capacity and interests of an employer. See Gossmeyer v. McDonald, 128 F.3d 481, 492-93 (7th Cir. 1997) (concluding that presence of law enforcement personnel at search of employee's office by government employer did not preclude application of O'Connor); see also 4 Wayne R. LaFave, Search and Seizure § 10.3(d), at 487-88 (3d ed. 1996) (noting that conclusion that warrant requirement does not apply when employer is investigating work-related criminal conduct is consistent with reasoning of O'Connor); cf. United States v. Nasser, 476 F.2d 1111, 1123-24 (7th Cir. 1973) (upholding as reasonable under the Fourth Amendment a government employer's electronic surveillance of an employee that yielded evidence of criminal misconduct, based upon the relationship of the search to the employee's work duties); cf. also Waters v. Churchill , 511 U.S. 661, 671 (1994) (plurality opinion) (stating that, in the First Amendment context, "the government as employer indeed has far broader powers than does the government as sovereign").

We have little trouble concluding that the warrantless entry of Simons' office was reasonable under the Fourth Amendment standard announced in O'Connor. At the inception of the search FBIS had "reasonable grounds for suspecting" that the hard drive would yield evidence of misconduct because FBIS was already aware that Simons had misused his Internet access to download over a thousand pornographic images, some of which involved minors. O'Connor, 480 U.S. at 726. The search was also permissible in scope. The measure adopted, entering Simons' office, was reasonably related to the objective of the search, retrieval of the hard drive. And, the search was not excessively intrusive. Indeed, there has been no suggestion that Harper searched Simons' desk or any other items in the office; rather,

Harper simply crossed the floor of Simons' office, switched hard drives, and exited.

In the final analysis, this case involves an employee's supervisor entering the employee's government office and retrieving a piece of government equipment in which the employee had absolutely no expectation of privacy--equipment that the employer knew contained evidence of crimes committed by the employee in the employee's office. This situation may be contrasted with one in which the criminal acts of a government employee were unrelated to his employment. Here, there was a conjunction of the conduct that violated the employer's policy and the conduct that violated the criminal law. We consider that FBIS' intrusion into Simons' office to retrieve the hard drive is one in which a reasonable employer might engage. See Vernonia Sch. Dist. 47J, 515 U.S. at 665 (characterizing the relevant question as whether the intrusion by the government employer is one in which a reasonable employer might engage).

For the foregoing reasons, we agree with the district court that Simons' Fourth Amendment rights were not violated by any of FBIS' activities in searching his computer and office.

III.

Simons also challenges the search conducted pursuant to the August search warrant. We reject Simons' arguments that the search violated his constitutional rights. However, we remand for further proceedings concerning Simons' claim that the search team violated Federal Rule of Criminal Procedure 41(d) when it failed to leave, at the time of the search, a copy of the warrant or a receipt for the property taken.

Simons first alleges that the warrant was invalid as to the zip drive and zip drive diskettes because the affidavit supporting the warrant application contained a deliberately misleading statement--that Simons had attached a zip drive to his computer. At the suppression hearing, Mauck stated that he did not know whether a zip drive was connected to Simons' computer, and Harper essentially testified that he did not believe there was a zip drive connected to Simons' computer. Because at least Harper participated in preparing the warrant

application, Simons attributes the knowledge of these SAIC employees to Mesisca, the author of the affidavit. Simons argues that the affidavit therefore contained a knowingly false statement and that the statement impermissibly expanded the scope of the search because without the statement there was no probable cause to search the zip drive or zip drive diskettes.

"[I]n all cases outside the exceptions to the warrant requirement the Fourth Amendment requires the interposition of a neutral and detached magistrate between the police and the persons, houses, papers, and effects of citizens." Thompson v. Louisiana, 469 U.S. 17, 20 (1984) (per curiam) (internal quotation marks omitted). In evaluating whether probable cause exists, it is the task of the issuing magistrate to decide "whether, given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). Information contained in the affidavit and critical to such a finding of probable cause must "be `truthful' in the sense that the information put forth is believed or appropriately accepted by the affiant as true." Franks v. Delaware, 438 U.S. 154, 165 (1978). However, to challenge the validity of the August search warrant on the ground that the supporting affidavit was not truthful, Simons must do more than simply make conclusory claims of a misstatement. Instead, he must show that Mesisca made the false statement either deliberately or with reckless disregard for its truth and that the statement was essential to the finding of probable cause. See id. at 171-72.

Simons has failed to satisfy these threshold requirements. He has introduced no evidence showing that Mesisca made the statement regarding the zip drive deliberately or with reckless disregard for the truth, nor has he shown that the statement was critical to the finding of probable cause. At most, the scope of the misstatement was that the zip drive was connected to the computer. As the magistrate judge found probable cause to search other items in the office not connected to the computer, whether the zip drive was actually connected to the computer was obviously not essential to the probable cause determination. We therefore conclude that the statement in the affidavit

regarding the zip drive being connected to the computer did not render the seizure of the zip drive and zip drive diskettes unlawful.**12**

Next, Simons argues that the August search violated the Fourth Amendment and Federal Rule of Criminal Procedure 41(d) because the search team executing the warrant left neither a copy of the warrant nor a receipt for the property taken. We conclude that these failings did not violate Simons' constitutional rights, but we remand for the district court to determine whether the executors of the warrant deliberately violated Rule 41(d).

Federal Rule of Criminal Procedure 41(d) provides, in pertinent part, that

> [t]he officer taking property under the warrant shall give to the person from whom or from whose premises the property was taken a copy of the warrant and a receipt for the property taken or shall leave the copy and receipt at the place from which the property was taken.

Fed. R. Crim. P. 41(d). The August search warrant stated substantially the same requirements. However, the search team that executed the warrant left neither a copy of the warrant nor a receipt for the property taken. Therefore, it is clear that the executors of the warrant violated Rule 41(d). Simons argues that the failure to leave notice of the search violated his Fourth Amendment rights and was a deliberate violation of Rule 41(d); he maintains that suppression is an appropriate remedy.

There are two categories of Rule 41 violations: those involving constitutional violations, and all others. See United States v. Chaar,

---

12 We reject the same argument with regard to the application for the September warrant. Simons also argues that the September application contained an additional knowing misrepresentation because the affidavit described the August application as one for a surreptitious search warrant. Regardless of whether there is any evidence that Mesisca made this statement deliberately, or with reckless disregard for the truth, there is no reason to suspect that the statement affected the probable cause determination.

137 F.3d 359, 362 (6th Cir. 1998); United States v. Gerber, 994 F.2d 1556, 1560 (11th Cir. 1993); United States v. Negrete-Gonzales, 966 F.2d 1277, 1283 (9th Cir. 1992); United States v. Burke, 517 F.2d 377, 386-87 (2d Cir. 1975). The violations termed"ministerial" in our prior cases obviously fall into the latter category. See United States v. Smith, 914 F.2d 565, 568 (4th Cir. 1990) (labeling as "ministerial" claimed error that government had not returned warrant to magistrate judge within prescribed period); United States v. Wyder, 674 F.2d 224, 225-26 (4th Cir. 1982) (labeling as "ministerial" scrivenor's error contained in copy of the warrant given to the defendant). Non-constitutional violations of Rule 41 warrant suppression only when the defendant is prejudiced by the violation, see Smith, 914 F.2d at 568; Wyder, 674 F.2d at 226, or when "there is evidence of intentional and deliberate disregard of a provision in the Rule," Burke, 517 F.2d at 387. See Chaar, 137 F.3d at 362; Gerber, 994 F.2d at 1560; Negrete-Gonzales, 966 F.2d at 1283.

First, we conclude that the failure of the team executing the warrant to leave either a copy of the warrant or a receipt for the items taken did not render the search unreasonable under the Fourth Amendment. The Fourth Amendment does not mention notice, and the Supreme Court has stated that the Constitution does not categorically proscribe covert entries, which necessarily involve a delay in notice. See Dalia v. United States, 441 U.S. 238, 247-48 (1979). And, insofar as the August search satisfied the requirements of the Fourth Amendment, i.e., it was conducted pursuant to a warrant based on probable cause issued by a neutral and detached magistrate, we perceive no basis for concluding that the 45-day delay in notice rendered the search unconstitutional. See United States v. Pangburn, 983 F.2d 449, 453-55 (2d Cir. 1993) (holding that the notice requirement found in Rule 41(d) is not required by the Fourth Amendment). But see United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986) (holding that search warrant was constitutionally defective because it did not require notice).

Having concluded that the Rule 41(d) violation at issue here did not infringe on Simons' constitutional rights, we must now evaluate his argument that the violation was deliberate. **13** As described above,

---

13 Simons does not maintain on appeal that he was prejudiced by the Rule 41(d) violation.

the affidavit supporting the August warrant application stated a "need" to conduct the search in secret. J.A. 140. However, the warrant required its executors to leave a copy of the warrant and a receipt for the property taken. Based on these facts, Simons argues that the search team applied for, but the magistrate judge denied, a warrant to conduct a secret search. Simons further maintains that the team deliberately circumvented the denial of its request when it failed to leave notice of the search. The Government responds that the search team applied for and believed that it had received a warrant that authorized a secret search.

The district court did not address the intent issue when it ruled on Simons' motion to suppress, and as a factual matter it is beyond our province on appeal. We therefore remand for the district court to consider whether the Government intentionally and deliberately disregarded the notice provision of Rule 41(d) when it carried out the August 6, 1998 search.

IV.

We conclude that FBIS' searches of Simons' computer and office did not violate Simons' Fourth Amendment rights. We also determine that the August search warrant was valid and that the violation of Rule 41(d) did not render the search constitutionally unreasonable. However, we remand for the district court to consider whether Rule 41(d) was intentionally and deliberately disregarded.

AFFIRMED IN PART, REMANDED IN PART